UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/519,827	12/21/2005	Michael Jacobs	CHAP-005	3097

36822 7590 06/16/2008

GORDON & JACOBSON, P.C.
60 LONG RIDGE ROAD
SUITE 407
STAMFORD, CT 06902

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
06/16/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/519,827	JACOBS, MICHAEL	
	Examiner	Art Unit	
	BRYAN WRIGHT	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *24-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *24-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 December 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10/11/2006, 10/11/2006, 9/26/2006,9/19/2006, 2/16/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action in response to application December 21, 2005. Claims (24-42) are pending.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 24-30 and 41 are rejected under 35 U.S.C. 102(b) as being anticipated by Farber et al. (US Patent No. 6,928,442 and Farber hereinafter).

3. As to claim 24, Farber teaches a **apparatus for storage of data comprising: means for storing copies of a plurality of data items** (i.e., Farber teaches storing files on a first computer in a network [col. 40, lines 40-50]), **means for generating at the end of a predetermined period of time** (i.e., Farber teaches a limited period of time [col. 30, lines 43-46]), **a data file comprising hash values of each data item created and/or stored during that time, means for generating a single hash value of said data file** (i.e., Farber teaches a data item based on a function (e.g., SHA) [abstract lines 6-10]), **and means for transmitting** (i.e., provided) **said single hash value to a remote location for storage** (i.e., parties) **or publication of the single hash value or publication of data representative thereof** (i.e., Farber

teaches publication capability [col. 30, lines 43-46] Farber teaches a providing said copy to parties thereof [abstract lines 11-12]).

4. As to claim 25, Farber teaches a **apparatus according where said data file comprises a hash value of each of the data items created or stored during said predetermined period of time together with one or more of a file name, a path name, the file size and a time-stamp in relation to each data item** (i.e., Farber teaches a data item based on a function (e.g., SHA) [abstract lines 6-10]).

5. As to claim 26, Farber teaches a **apparatus according where at said remote location, a second data file is created** (i.e., copy) **comprising said single hash value and one or more additional data items relating to said single hash value, and a single hash value, and a single hash value, said second data file being stored or published** (i.e., Farber teaches publication capability [col. 30, lines 43-46] Farber teaches a providing said copy to parties thereof [abstract lines 11-12]).

6. As to claim 27, Farber teaches a method of storing and authenticating data, comprising the steps of:

storing copies of a plurality of data items (i.e., Farber teaches storing files on a first computer in a network [col. 40, lines 40-50]), **generating at the end of a predetermined period of time** (i.e., Farber teaches a limited period of time [col. 30, lines 43-46]), **a data file comprising hash values of each data item created and/or**

signed during that time, generating a single hash value of said data file (i.e., Farber teaches a data item based on a function (e.g., SHA) [abstract lines 6-10]), **and transmitting** (i.e., provided) **said single hash value to a remote location for storage** (i.e., parties) **of the single hash value or publication of the single hash value or publication thereof** (i.e., Farber teaches publication capability [col. 30, lines 43-46] Farber teaches a transmitting said copy to parties thereof [abstract lines 11-12]).

7. As to claim 28, Farber teaches a method **further comprising the steps of: creating a second data file comprising said single hash value and one or more data items relating thereto** (i.e., Farber teaches data item based on a function (i.e., SHA) [abstract, lines 6-10]), **and creating a single hash value of said second data file for storage or publication** (i.e., Farber teaches a copy of the data item is provided to parties thereof [abstract, lines 11-13] Farber teaches publication capability [col. 30, lines 43-46]).

8. As to claim 29, Farber teaches a **method further comprising the steps of: retrieving a stored set of data items for a predetermined time period** (i.e., Farber teaches a retrieving data items [col. 6, lines 15 -20] Farber teaches a retrieval request for a period for which said period corresponds to a timeout period [col. 16, lines 19-25]), **generating a data file comprising the hash values of each of said data items (i.e., Farber teaches computing the said data item** (i.e., True Name) using a MD function (i.e., hash function) [col. 12, lines 55-65]), **and comparing one or more of said hash**

values (i.e. True Name) **with the corresponding hash value or values sin the data file generated in claim 27 to determine whether or not they match** (i.e., Farber teaches comparing the hash value (i.e., True Name) for a match [col. 15, line 26-32]).

9. As to claim 30, Farber teaches a method **further comprising the steps of: generating a single hash value of the data file** (i.e., data item) **generated in claim 29** (i.e., Farber teaches utilizing a MD function (i.e., hash function) to generate a hash of a data item [col. 13, lines 1-5; lines 12-17]), **and comparing it with the corresponding single hash value generated in claim 27, to determine whether or not they match** (i.e., Farber teaches comparing the hash value (i.e., True Name) for a match [col. 15, line 26-32]).

10. As to claim 41, Farber teaches a **apparatus for verifying by a second end user the authenticity of use of an identifier by a first end user, the apparatus comprising: means for identifying the communication of a data item encrypted using or otherwise including an identifier unique to said first end user from said first end user to said second end user across an information technology communications network** (i.e., Farber teaches use of a “True Name" for which is a unique identifier for a particular data item [col. 6, 5-11] Farber teaches a function (i.e., MD4, MD5) for which the is used in data authentication [col. 15, lines 12-17] One of ordinary skill in the art would recognize the (MD4) as a cryptology practice [col. 13, lines 40-50]), **means for accessing** (i.e., Farber teaches a region table for which access

rules are define [par. 8, lines 20-45]), **in response to such identification, storage** (i.e., audit file) **means containing information relating to one or more valid recent events or transactions** (i.e., changes) **relating to said identifier which have occurred across said information technology communications network** (i.e., Farber teaches use of a audit file indicating changes [col. 8, lines 45-55]) , **means for obtaining confirmation** (i.e., license) **from said first end user that at least one of said recent events or transactions** (i.e., user authorized to access) **is valid** (i.e., Farber teaches the use of licenses to determine if user has access authorization [par. 12, lines 5-12]), **and means for preventing further use of said identifier in the event that such confirmation is not received** (i.e., Farber teaches a preventative means for which a user is not confirmed as a authorized [col. 32, lines 40-51]).

11. Claims 31, 37, 38, 39, and 42 are rejected under 35 U.S.C. 102(e) as being anticipated by Olkin et al. (US Patent No. 6,584,564 and Olkin hereinafter).

12. As to claim 31, Olkin teaches a **apparatus for transmitting data between first and second end users via an information technology communications network** [fig. 1], **said first end user comprising means for encrypting a data item using a first identifier** (i.e., message key) (i.e., Olkin teaches a encrypting message with message key [abstract, lines 1-12]), **and transmitting said encrypted data item to said second end user** [abstract; fig. 1], **said second end user comprising means for receiving said encrypted data item and transmitting an acknowledgement signal**

to said first end user [col. 13, lines 53 -67; col. 14, lines 1-10], **said first end user further comprising means for encrypting said first identifier** (i.e., message key) **using a second identifier** (i.e., public key) (i.e., Olkin teaches encrypting message key with public key [col. 17, lines 35-36]) **and transmitting** (i.e., sending) **said encrypted first identifier** (i.e., message key) **to said second end user in response to receipt of said acknowledgement signal** [col. 13, lines 53 -67; col. 14, lines 1-10], **said second end user further comprising means for requesting and receiving said second identifier** (i.e., public key) **in response to receipt of said encrypted first identifier** (i.e., Olkin teaches means for the key to be accessible [col. 17, lines 48-49]), and **means for decrypting said first identifier using said second identifier and for decrypting said data item using said first identifier** (i.e., Olkin teaches decrypting secure e-mail (i.e., data item) with message key (i.e., first identifier and second identifier [col. 16, lines 29-31]).

13. As to claim 37, Olkin teaches a **apparatus where the data item is encrypted using a symmetric key and the first identifier or key is encrypted using an asymmetric Key** (i.e., Olkin teaches a use of a message key for which is symmetric [col., 17, lines 29-30]).

14. As to claim 38, Olkin teaches a **apparatus where the acknowledgement signal comprises an encrypted or compressed version** (i.e., hash) **of the original data ite**m [col. 17, lines 60-67; col. 18, lines 1-10].

15. As to claim 39, Olkin teaches a **apparatus where the encrypted or compressed version of the original data item is a hash value thereof** [col. 17, lines 60-67; col. 18, lines 1-10].

16. As to claim 42, Olkin teaches a **method for verifying by a second end user the authenticity of use of an identifier by a first end user, the method comprising the steps of:**

Identifying (i.e., Olkin teaches the act of authenticating a sender)**the communication of a data item** (i.e., secure email) **encrypted using or otherwise including an identifier unique** (i.e., message key) **to said first end user from said first end user to said second end user across an information technology communications network** (e.g., SSL) (i.e., Olkin teaches a sending a request to a security server via to authenticate a sender and obtain message key for use to encrypt the secure e-mail [col. 11, lines 59-67]), **accessing** (i.e., creates and populates), in **response to such identification** [col. 13, lines 50-55], **storage means** (i.e., sentMail table) **containing information relating to one or more valid recent events or transactions relating to said identifier which have occurred across said information technology communications network** (i.e., Olkin teaches creating and populating a sentMail table [col. 13, lines 53-67]), **obtaining confirmation from said first end user that at least one of said recent events or transactions is valid** [col. 14, lines 1-5], **and preventing further use** (i.e., destroy key) **of said identifier** (i.e.

message key) **in the event that such confirmation is not received** (col. 14, lines 5-10]).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

17. Claims 32, 33, and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Olkin in view of Boneh et al. (US Patent No. 7,113,594 and Boneh hereinafter).

18. As to claims 32, 33, and 36 the system disclosed by Olkin shows substantial features of the claimed invention (discussed in the paragraph above), it fails to disclose:

An apparatus where the second identifier is stored remotely from said first and second end users (claim 32).

A apparatus where the second identifier is stored by a third party (claim 33).

A apparatus where a request for the second identifier (i.e., key) **is sent to said remote storage location, the request being in the form of the**

encrypted data item or an encrypted version of the first identifier (claim 36) (to provide a third party key control [col. 30, line 25-60]).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Olkin as introduced by Boneh. Boneh discloses:

An apparatus where the second identifier (i.e., key) **is stored remotely from said first and second end users** (claim 32) (to provide remote key storage [col. 30, line 25-60]).

A apparatus where the second identifier is stored by a third party (claim 33) (to provide third party key storage capability [col. 30, line 25-60]).

A apparatus where a request for the second identifier (i.e., key) **is sent to said remote storage location, the request being in the form of the encrypted data item or an encrypted version of the first identifier** (claim 36) (to provide a third party key control [col. 30, line 25-60]).

Therefore, given the teachings of Boneh, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Olkin by employing the well known feature of remote key storage disclosed above by Boneh, for which authentication will be enhanced [col. 30, line 25-60].

19. As to claim 40, Olkin teaches a **method for transmitting data between first and second end users via an information technology communications network, comprising the steps of:**

encrypting by the first end user a data item using a first identifier and transmitting said encrypted data item to said second end user [fig. 1], receiving by said second end user said encrypted data item and transmitting an acknowledgement signal to said first end user**, said first end user encrypting said first identifier** (i.e., message key) **using a second identifier** (i.e., public key) (i.e., Olkin teaches encrypting message key with public key [col. 17, lines 35-36]) and transmitting said encrypted first identifier to said second end user in response to receipt of said acknowledgement signal,

However Olkin does not expressly teach:

said second end user requesting and receiving said second identifier in response to receipt of said encrypted first identifier, decrypting said first identifier using said second identifier and decrypting said data item using said first identifier

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Olkin as introduced by Boneh. Boneh discloses:

said second end user requesting and receiving said second identifier in response to receipt of said encrypted first identifier (to provide third party key storage capability [col. 30, line 25-60])**, decrypting said first identifier using said second identifier and decrypting said data item** (i.e., original message) **using said first identifier** (i.e., decryption key) (to provide decryption capability using decryption key obtained from third party [col. 30, line 50-60]).

Therefore, given the teachings of Boneh, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Olkin by employing the well known feature of remote key storage and decryption disclosed above by Boneh, for which authentication will be enhanced [col. 30, line 25-60].

20. Claims 34 and 35, are rejected under 35 U.S.C. 103(a) as being unpatentable over Olkin in view of Boneh as applied to claim 32 above, and further in view of Okamoto et al. (US Patent No. 6,118,874 and Okamoto hereinafter).

21. As to claim 34 the system disclosed by Olkin in view of Boneh shows substantial features of the claimed invention (discussed in the paragraph above), it fails to disclose:

A apparatus where said second identifier is transmitted to said remote storage location by said first end user in response to commencement of a data transfer transaction thereby (claim 34).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Olkin in view of Boneh as introduced by Okamoto. Okamoto discloses:

A apparatus where said second identifier is transmitted to said remote storage location by said first end user in response to commencement of a data transfer transaction thereby (claim 34) (to provide second identifier storage capability [claim 8, lines 5-15].

Therefore, given the teachings of Okamoto, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Olkin in view of Boneh by employing the well known feature of second identifier storage disclosed above by Okamoto, for which authentication will be enhanced [claim 8, lines 5-15].

22. As to claim 35, Olkin teaches a **apparatus where the transaction embodied by transmission of a second identifier** (i.e., key) **to the remote storage location** (i.e., security server) **is time stamped** (i.e., Olkin teaches a expiration setting [col. 9, lines 25-27]).

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2131
/Ayaz R. Sheikh/

Supervisory Patent Examiner, Art Unit 2131